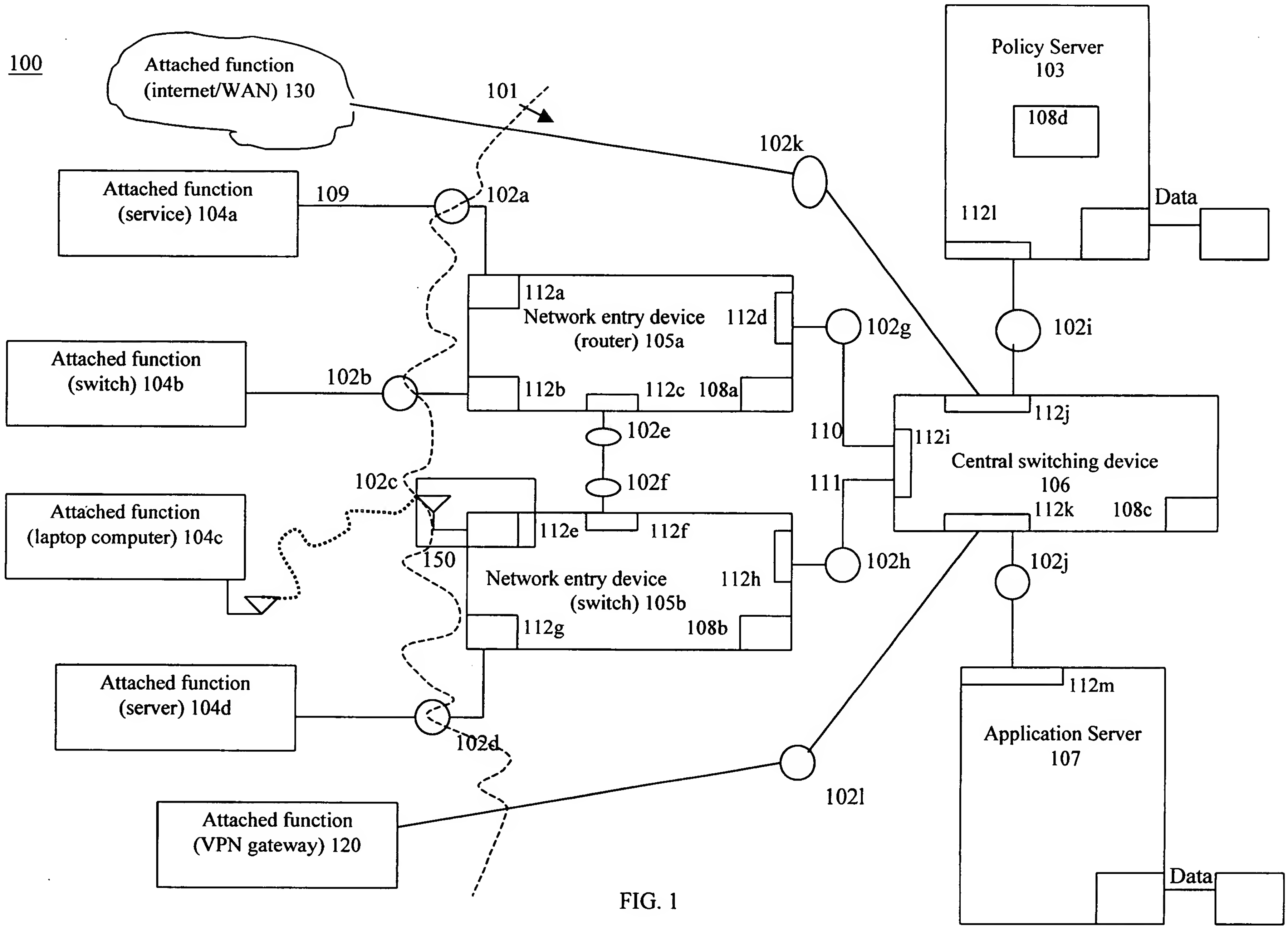

100
Attached function (internet/WAN) 130
101
102k
Policy Server 103
108d
112l
Data
Attached function (service) 104a
109
102a
112a
Network entry device (router) 105a
112d
102g
102i
Attached function (switch) 104b
102b
112b
112c
108a
112j
102e
110
112i
Central switching device 106
102c
102f
111
Attached function (laptop computer) 104c
112e
112f
112k
108c
150
Network entry device (switch) 105b
112h
102h
102j
112g
108b
Attached function (server) 104d
102d
112m
Application Server 107
102l
Attached function (VPN gateway) 120
Data

FIG. 1

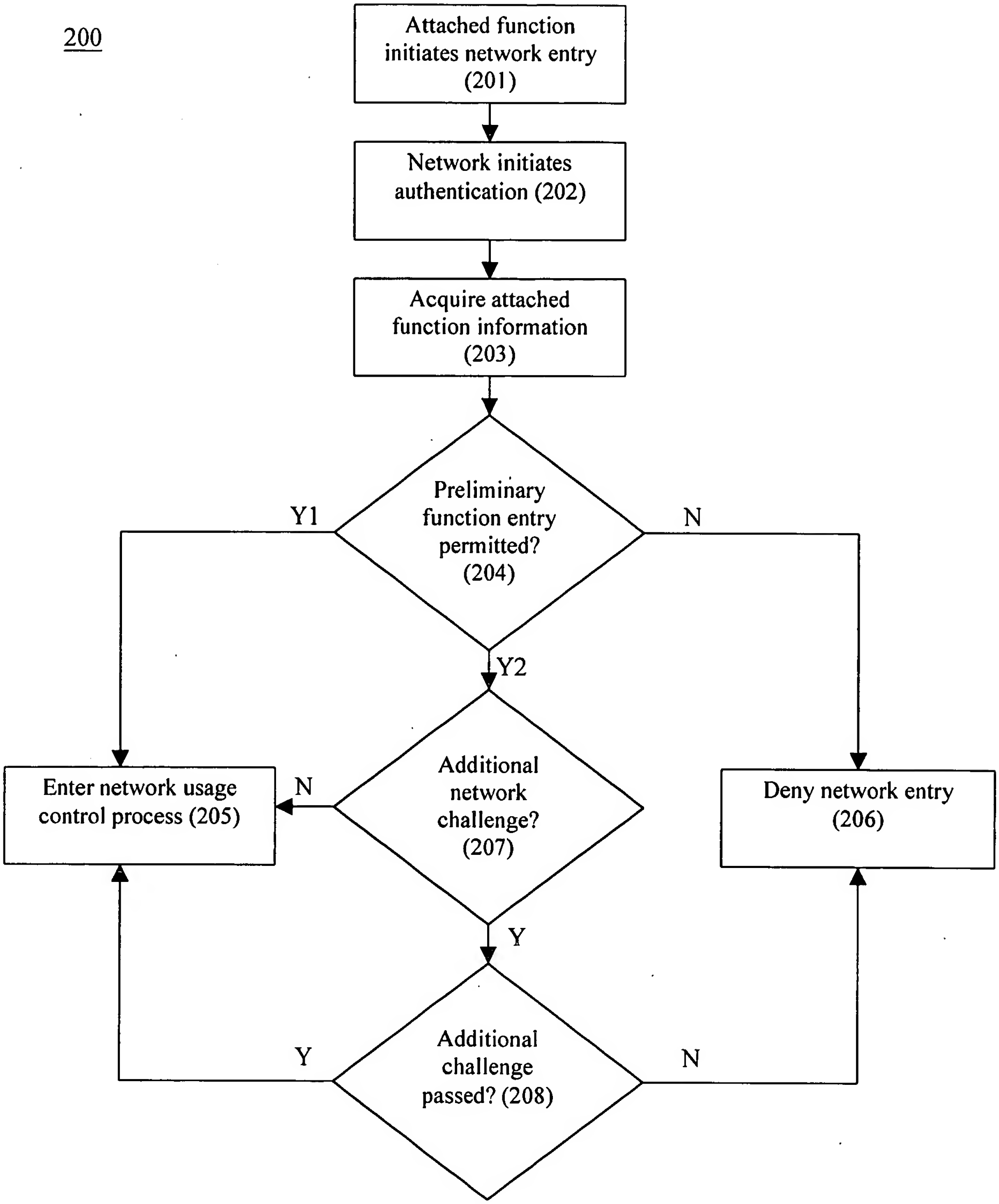
200
Attached function initiates network entry (201)
Network initiates authentication (202)
Acquire attached function information (203)
Preliminary function entry permitted? (204)
Y1
N
Y2
Additional network challenge? (207)
N
Enter network usage control process (205)
Deny network entry (206)
Y
Additional challenge passed? (208)
Y
N

FIG. 2

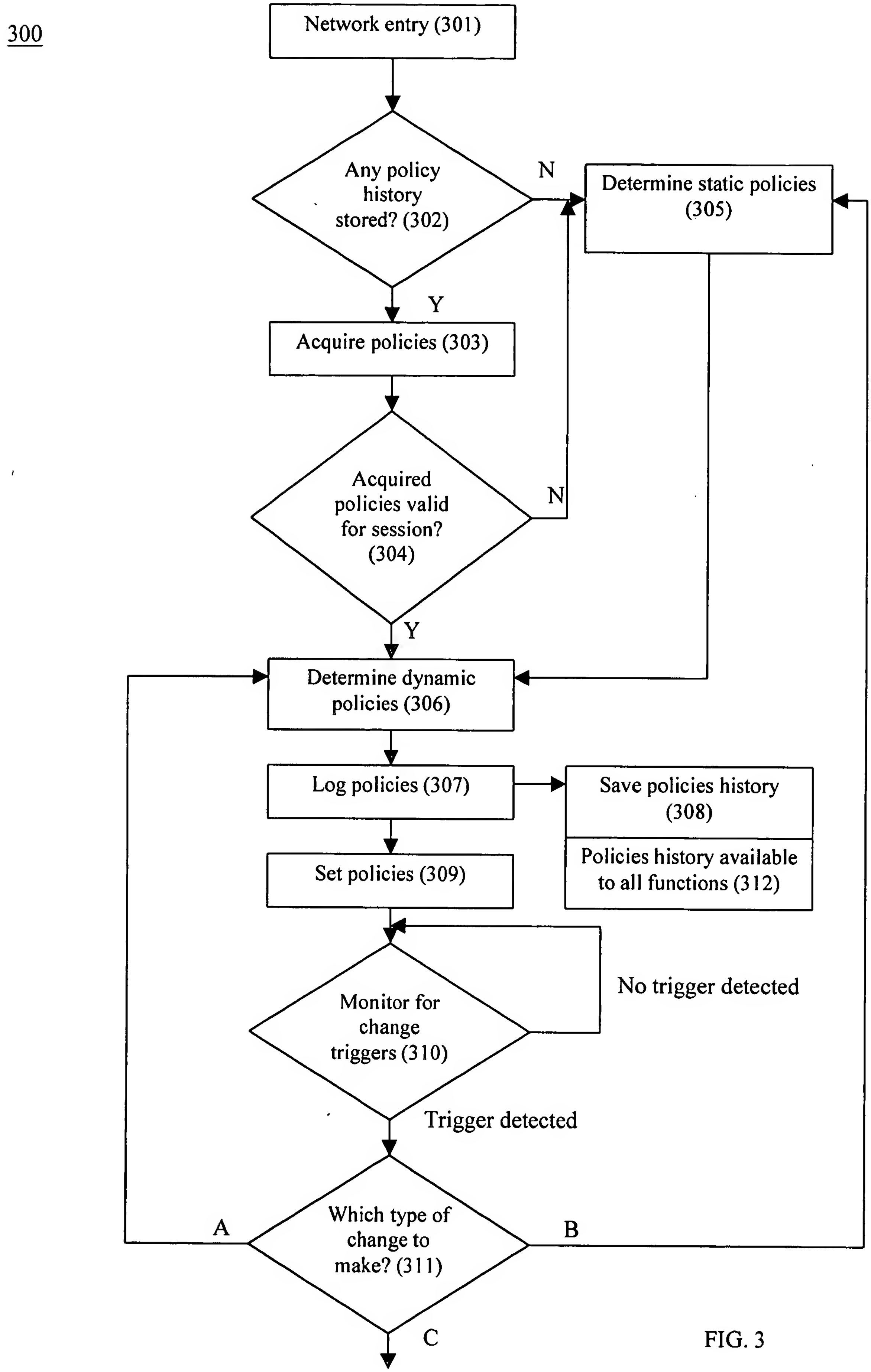
300
Network entry (301)
Any policy history stored? (302)
N
Determine static policies (305)
Y
Acquire policies (303)
Acquired policies valid for session? (304)
N
Y
Determine dynamic policies (306)
Log policies (307)
Save policies history (308)
Policies history available to all functions (312)
Set policies (309)
Monitor for change triggers (310)
No trigger detected
Trigger detected
Which type of change to make? (311)
A
B
C

FIG. 3

Information	**Change triggers**	**Policies**
User ID	Time Outs	Internet Access Only
Device type	Link Changes, up/down, speed	IEEE 802.1X Authentication Required
Device Location	User Changes	Disable Unused Ports
Access Device	Device Changes	Reset On Intrusion Detection
Access Location	Device Additions	Specific Application Access Only
Port Type and Speed	Network Service Changes	Priority Access
Users Per Port	Access Device Changes	Application Bandwidth Limits
Devices Per Port	Location Changes	Port Based Priority
Devices Per User	IDS or Firewall Events	L2 Protocol Filter/Access List
Time Of Access	Application Access Request	Multi-step authentication
Application Used	Priority Change Request	Wireless/Wired Access Rules
Application Priority	Protocol Change	Log All Traffic
Port Security	Additional Wireless User	Set Group Characteristic Rules
Requested Priority	Administrator Set Policy Changes	New Session Logging
Ethernet Protocol	Bandwidth Changes	Flow Logging
Level of Trust	Routing Link Cost Changes	Limit Port Setting (speed, priority, ACL)
Virus Scan level	RMON or Other Monitored Events	Phone Access Only
Operating System Type and Version	Dynamic Policy Changes (local)	Time-of-Day Based Access (any policy)
Network system	Dynamic Policy Changes (remote)	Stateful Inspection
	Network system changes	

FIG. 4